UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF GEORGIA

JAMES BYRNE, individually and on behalf of all others similarly situated, Plaintiff, -v- AFLAC INCORPORATED, Defendant.	Case No.: **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiff James Byrne, individually and on behalf of all others similarly situated ("Class" or "Class Members"), bring this Class Action Complaint ("Complaint") against Defendant AFLAC Incorporated ("AFLAC" or "Defendant"). The allegations set forth in this Complaint are based on the knowledge of Plaintiff and upon information and belief and further investigation of counsel.

NATURE OF THE ACTION

1. This class action arises out of the recent cyberattack and data breach resulting from Defendant's failure to implement reasonable and industry standard security practices[1].

2. Defendant is a Fortune 500 company providing insurance products to millions of policyholders and customers through its subsidiaries in the U.S. and is one of the

[1] *See* Exhibit A, Plaintiff's Notice Email.

largest suppliers of supplemental health insurance in the United States for medical expenses that are not covered by a primary provider.[2]

3. As a provider of insurance services, AFLAC knowingly obtains sensitive customer and information and has a resulting duty to maintain such information in confidence. The company has sensitive information concerning over 50 million customers in the U.S. and abroad.[3]

4. Plaintiffs bring this Complaint against Defendant for its failure to properly secure and safeguard the sensitive information that it collected and maintained as part of its regular business practices, including, but not limited to: names; demographic information, such as addresses, emails, and phone numbers ("Personally Identifying Information" or "Private Information") and medical treatment and insurance information, which is protected health information ("PHI") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") (collectively with PII, "Private Information").

5. Upon information and belief, former and current customers of Defendant are required to entrust Defendant with sensitive, non-public "Private Information", without which Defendant could not perform its regular business activities, to obtain health insurance from Defendant.

---

[2] https://www.aflac.com/about-aflac (last accessed June 20, 2025).
[3] https://healthexec.com/topics/health-it/cybersecurity/health-data-possibly-exposed-sophisticated-cyberattack-aflac(last accessed June 23, 2025).

6. By obtaining, collecting, using, and deriving a benefit from the "Private Information" of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

7. As discussed in more detail below, AFLAC breached its duty to protect the "Private Information" entrusted to it.

8. AFLAC announced on June 20, 2025 that on June 12, 2025 AFLAC identified suspicious activity on its network in the United States that potentially impacted files containing "claims information, health information, social security numbers, and/or other personal information, related to customers, beneficiaries, employees, agents, and other individuals in our U.S. business"[4] (the "Data Breach").

9. The Data Breach involved unauthorized access to customers' "Private Information" as part of a hacking spree against U.S. insurance companies by the cybercrime group known as "Scattered Spider." [5]

10. On June 20, 2025, AFLAC said it did not know how much customer information may have been stolen in the Data Breach but that the potential exposure is "vast."[6]

---

[4] https://newsroom.aflac.com/2025-06-20-Aflac-Incorporated-Discloses-Cybersecurity-Incident(last accessed June 20, 2025).
[5] *See* https://www.cnn.com/2025/06/20/tech/aflac-cyberattack#:~:text=Cybercriminals%20have%20breached%20insurance%20giant,hacks%20against%20the%20insurance%20industry. (last accessed June 20, 2025).
[6] *Id*.

11. AFLAC stated on June 20, 2025, that AFLAC "commenced a review of potentially impacted files" but that "the review is in its early stages, and [AFLAC is] unable to determine the total number of affected individuals until that review is completed."[7]

12. Defendant failed to adequately protect Plaintiff's and Class Members' "Private Information". This "Private Information" was compromised due to Defendant's negligent and/or careless acts and omissions and their utter failure to protect its customers' sensitive data. Hackers targeted and obtained Plaintiffs' and Class Members' "Private Information" because of its value in exploiting and stealing the identities of Plaintiffs and Class Members. The present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

13. "Scattered Spider" is a notorious cybercriminal group that "targets large companies and their contracted information technology (IT) help desks. Scattered Spider threat actors, per trusted third parties, have typically engaged in data theft for extortion and have also been known to utilize BlackCat/ALPHV ransomware alongside their usual TTPs."[8] Plaintiff and Class Members' sensitive data is now unquestionably in the hands of malicious actors who specialize in identity theft and fraud.

[7] *See* https://newsroom.aflac.com/2025-06-20-Aflac-Incorporated-Discloses-Cybersecurity-Incident
[8] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a(last accessed June 22, 2025).

14. As discussed in more detail below, as a result of its inadequate data security and in breaching its duties to properly safeguard its customers' "Private Information", Defendant has violated federal and state regulations and caused its customers imminent and ongoing risk of harm.

15. Plaintiff is now at a significantly increased and certainly impending risk of fraud, identity theft, misappropriation of health insurance benefits, intrusion of privacy and similar forms of criminal harm.

16. Plaintiffs bring this action on behalf of all persons whose Private Information was compromised as a result of Defendant's failure to: (i) adequately protect the Private Information of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected Private Information using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts at least to negligence and violates federal and state statutes.

17. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to implement and maintain adequate and reasonable measures to ensure that the Private Information of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and

appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the Private Information of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

18. Plaintiff brings this action on behalf of all persons whose "Private Information" was compromised as a result of Defendant's conduct. Specifically, Plaintiff brings claims for negligence, negligence per se, breach of fiduciary duty, breach of an implied contract unjust enrichment, and declaratory judgment, seeking actual and punitive damages, with attorneys' fees, costs, and expenses, and appropriate injunctive and declaratory relief.

19. Plaintiff seeks to remedy these harms and prevent any future data compromise on behalf of himself and all similarly situated persons whose personal data was compromised and stolen as a result of the Data Breach and who remain at risk due to Defendant's inadequate security practices.

PARTIES

20. Plaintiff James Byrne is and has been, at all relevant times, a resident and citizen of New York, residing in Queens, New York with intent to remain.

21. At all relevant times herein, Defendant has been a resident and citizen of Georgia, with its principal office located at 1932 Wynnton Road, Columbus, Georgia, 31999.

JURISDICTION AND VENUE

22. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1332(d). The amount in controversy in this Class action exceeds $5,000,000, exclusive of interest and costs, and there are numerous Class members who are citizens of states other than Defendant's state of citizenship, including Plaintiff, who is a citizen of New York.

23. This Court has personal jurisdiction over Defendant as Defendant is incorporated in this District, has substantial contacts with this District, and transacts business in this District.

24. Venue is proper in this District under 28 U.S.C. §1391(b) because AFLAC is deemed to reside in this District because Defendant is subject to the Court's personal jurisdiction with respect to this Action and because a substantial part of the events giving rise to the claims herein occurred in this District, and Defendant regularly conducts business in this District.

STATEMENT OF FACTS

Defendant's Business

25. As stated above, Defendant is a Fortune 500 company that provides supplemental insurance to millions of customers in the United States and abroad.

26. In order to obtain insurance coverage from the Defendant, AFLAC requires that its customers provide sensitive and confidential Private Information including their names, contact information, social security numbers, and/or other personal information, including claims and health information.

27. Upon information and belief, Defendant made promises and representations to its customers that the Private Information collected from them would be kept safe, confidential, that the privacy of that information would be maintained, and that Defendant would delete any sensitive information after it was no longer required to maintain it.

28. Plaintiffs and Class Members provided their Private Information to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

29. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information. Plaintiffs and Class Members relied on the sophistication of Defendant to keep their Private Information confidential and securely maintained, to use this information for necessary purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members value the confidentiality of their Private Information and demand security to safeguard their Private Information.

30. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiffs and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep its customers' Private Information safe and confidential.

31. Defendant derived a substantial economic benefit from collecting Plaintiffs' and Class Members' Private Information. Without the required submission of Private Information, Defendant could not perform the services it provides.

32. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' Private Information from disclosure in the Data Breach.

The Data Breach

33. On or about June 20, 2025, AFLAC announced that it experienced a security incident that "potentially impacted files contain claims information, health information, social security numbers, and/or other personal information, related to customers, beneficiaries, employees, agents, and other individuals in [AFLAC's] U.S. business."[9]

[9] *See* https://newsroom.aflac.com/2025-06-20-Aflac-Incorporated-Discloses-Cybersecurity-Incident (last accessed June 20, 2025).

34. The breach occurred when a ransomware group penetrated AFLAC's information network(s). Since the Data Breach, AFLAC has failed to disclose whether it paid any ransom.

35. Like Plaintiff, other potential Class members received similar notices informing them of the Data Breach.

36. The Data Breach occurred as a direct result of Defendant's failure to implement and follow basic security procedures to protect its customers' and employees' Private Information.

Defendants Failed to Comply with FTC Guidelines

37. AFLAC is prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

38. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

39. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of

personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[10]

40. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[11]

41. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

42. AFLAC failed to properly implement basic data security practices. AFLAC's failure to employ reasonable and appropriate measures to protect against unauthorized access to patient Private Information constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

[10] *See* https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (last accessed June 20, 2025).
[11] *Id*.

43. AFLAC was at all times fully aware of its obligations to protect customers' Private Information. Defendant is also aware of the significant repercussions that would result from its failure to do so.

AFLAC Knew the Risks of Storing Valuable Personal Information

44. At all relevant times, AFLAC knew it was storing sensitive Private Information and that, as a result, its systems would be an attractive target for cybercriminals.

45. AFLAC also knew that a breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the individuals whose Private Information was compromised, as well as intrusion into their highly private information.

46. Moreover, AFLAC should have been aware that the financial services industry has become a prime target for cybercriminals and thus, alerted to its susceptibility to cyberattack, and taken proactive measures to enhance its data security.[12]

47. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack.

[12] *See* https://www.syteca.com/en/blog/data-protection-compliance-insurance-industry (last accessed June 20, 2025).

48. For example, in 2023, the number of data compromises in the United States stood at 3,205 cases, affecting over 353 million individuals.[13]

49. The type and breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendant's customers especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

50. PII is a valuable property right[14] and its value is measurable. American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[15] It is so valuable to identity thieves that once Private Information has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

51. As a result of their real value and the recent large-scale data breaches, identity thieves and cybercriminals have openly posted credit card numbers, Social Security numbers, PII, and other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated, and becomes more valuable to thieves and more damaging to victims.

---

[13] *See* https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ (last accessed June 20, 2025).
[14] *See* https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible") (last accessed June 20, 2025).
[15] *See* https://www.iab.com/news/2018-state-of-data-report/ (last accessed June 20, 2025).

52. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm."[16]

53. Even if stolen PII does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

54. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' Private Information has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

[16] *See* United States Government Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/new.items/d07737.pdf (last accessed June 15, 2025).

55. Based on the value of its customers' and employees' Private Information to cybercriminals and cybercriminals' propensity to target businesses, AFLAC certainly knew the foreseeable risk of failing to implement adequate cybersecurity measures.

Data Breaches Put Consumers at an Increased and Ongoing Risk of Fraud and Identity Theft

56. Cyberattacks and data breaches at companies that store Private Information are especially problematic because they can negatively impact on the overall daily lives of individuals affected by the attack.

57. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[17]

58. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, and to take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle,

[17] *See* https://www.gao.gov/products/gao-07-737 (last accessed June 20, 2025).

the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

59. Theft of Private Information is serious. The FTC warns consumers that identity thieves use Private Information to exhaust financial accounts, receive medical treatment, open new utility accounts, and incur charges and credit in a person's name.

60. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing freezes on their credit, and correcting their credit reports.[18]

[18] *See* https://www.identitytheft.gov/Steps (last accessed June 20, 2025).

61. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. Personal information is valuable to identity thieves, and if they can get access to it, they will use it to among other things: open a new credit card or loan, change a billing address so the victim no longer receives bills, open new utilities, obtain a mobile phone, open a bank account and write bad checks, use a debit card number to withdraw funds, obtain a new driver's license or ID, and/or use the victim's information in the event of arrest or court action.

62. Identity thieves can also use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, and/or rent a house or receive medical services in the victim's name.

63. Moreover, theft of Private Information is also gravely serious because Private Information is an extremely valuable property right.

64. Drug manufacturers, medical device manufacturers, pharmacies, hospitals, and other healthcare service providers often purchase Private Information on the black market for the purpose of target-marketing their products and services to the physical maladies of data breach victims themselves.

65.Each year, identity theft causes tens of billions of dollars of losses to victims in the United States. For example, with the Private Information stolen in the Data Breach, which includes Social Security numbers, identity thieves can open financial accounts, commit medical fraud, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft. These criminal activities have and will result in devastating financial and personal losses to Plaintiff.

66. As discussed above, Private Information is such a valuable commodity to identity thieves, and once the information has been compromised, criminals often trade the information on the "cyber black- market" for years.

67. Social Security numbers are particularly sensitive pieces of personal information. For instance, with a stolen Social Security number, which is only one subset of the Private Information compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits. Identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may be undetected until debt collection calls commence months, or even years later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment

benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected because one was already filed on their behalf.

68. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as the credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number.

69. This was a financially motivated Data Breach, as the only reason the cybercriminals go through the trouble of running a targeted cyberattack against companies like AFLAC is to get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein. This data demands a much higher price on the black market.

70. Fraud and identity theft resulting from the Data Breach may go undetected until debt collection calls commence months, or even years later. As with income tax returns, an individual may not know that his or her Social Security number was used

to file for unemployment benefits until law enforcement notified the individual's employer of the suspected fraud.

71. Cybercriminals can post stolen Private Information on the cyber black-market for years following a data breach, thereby making such information publicly available. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.

72. It is within this context that Plaintiff must now live with the knowledge that Plaintiff's Private Information is forever in cyberspace and was taken by people willing to use the information for any number of improper purposes and scams, including making the information available for sale on the black market.

73. Plaintiff must now take the time and effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on Plaintiff's everyday life, including purchasing identity theft and credit monitoring services every year for the rest of Plaintiff's life, placing "freezes" and "alerts" with credit reporting agencies, contacting his financial institutions and healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

74. Moreover, Plaintiff and Class members have an interest in ensuring that their Private Information, which remains in the possession of AFLAC, is protected from further public disclosure by the implementation of better employee training and industry standard and statutorily compliant security measures and safeguards. AFLAC has shown itself to be wholly incapable of protecting Plaintiff's Private Information.

75. Plaintiff and Class members also have an interest in ensuring that their personal information that was provided to AFLAC is removed from AFLAC's unencrypted files.

Plaintiff and the Class Suffered Damages

Facts Relevant To Plaintiff

76. AFLAC received Plaintiff's Private Information in connection with Plaintiff's application for insurance. In requesting and maintaining Plaintiff's Private Information for business purposes, AFLAC expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiff's and Class members' Private Information. AFLAC did not, however, take proper care of Plaintiff's and Class members' Private Information, leading to its exposure to and exfiltration by cybercriminals as a direct result of AFLAC's inadequate security measures.

77. In June 2025, Plaintiff received an alert in his AFLAC online account notifying him of a cybersecurity incident ("Notice").

78. Upon receiving the Notice, Plaintiff spent time reviewing his credit reports, reviewing various credit alerts received by text and email, checking his financial information, and dealing with increased spam text messages and emails.

79. Plaintiff has suffered imminent and impending injury arising from the present and ongoing risk of fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of unauthorized third parties and possibly criminals. Plaintiff suffered lost time, annoyance, interference, and inconvenience because of the Data Breach.

80. Plaintiff has experienced anxiety and increased concerns arising from the fact that his PII has been or will be misused and from the loss of his privacy.

81. The risk is not hypothetical, as cybercriminals intentionally stole the data, misused it, threatened to publish, or have published it on the Dark Web, and the sensitive information, including names and Social Security numbers, which is the type of PII used to perpetrate identity theft or fraud.

82. Plaintiff further suffered actual injury in the form of damages to and diminution in the value of his Private Information —a form of intangible property that he entrusted to Defendant, which was compromised in and because of the Data Breach.

83. Future identity theft monitoring is reasonable and necessary, and such services will include future costs and expenses.

84. Plaintiff has a continuing interest in ensuring that his Private Information which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff's And Class Members' Damages

85. For the reasons mentioned above, AFLAC's conduct, which allowed the Data Breach to occur, caused Plaintiff and Class members significant injuries and harm in several ways. Plaintiff and Class members must immediately devote time, energy, and money to: 1) closely monitor their medical statements, bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them. Plaintiff and Class members have taken or will be forced to take these measures in order to mitigate their potential damages as a result of the Data Breach.

86. Once Private Information is exposed, there is little that can be done to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiff and Class members will need to maintain these heightened measures for years, and possibly their entire lives as a result of Defendant's conduct.

87. As a result of Defendant's failures, Plaintiff and Class members are also at substantial and certainly impending increased risk of suffering identity theft and fraud or misuse of their PII.

88. Plaintiff is also at a continued risk because Plaintiff's information remains in AFLAC's computer systems, which have already been shown to be susceptible to compromise and attack and are subject to further attacks so long as AFLAC fails to undertake the necessary and appropriate security and training measures to protect its customers' Private Information.

89. In addition, Plaintiff and Class members have suffered emotional distress as a result of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private medical information to strangers.

CLASS ALLEGATIONS

90. Plaintiff brings all counts, as set forth below, individually and as a Class action, pursuant to the provisions of the Fed. R. Civ. P. 23, on behalf of a Class defined as:

> All individuals within the United States of America whose Private Information and/or financial information was exposed to unauthorized third-parties as a result of the Data Breach experienced by Defendant including all who received a Notice of the Data Breach in June 2025 (the "Class").

91. Excluded from the Class are Defendant, its subsidiaries and affiliates, officers and directors, any entity in which Defendant has a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial

officer(s) to whom this action is assigned, and the members of their immediate families.

92. Plaintiff hereby reserves the right to amend or modify the Class definition with greater specificity or division after having had an opportunity to conduct discovery.

93. Numerosity – The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class members is unknown to Plaintiff at this time, upon information and belief, there are at minimum, over a thousand members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through AFLAC's records, including but not limited to the files implicated in the Data Breach.

94. Commonality –This action involves questions of law and fact common to the Class. Such common questions include, but are not limited to:

a. Whether AFLAC had a duty to protect Plaintiff's and Class members Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

f. Whether AFLAC was negligent in collecting and storing Plaintiff's and Class members' Private Information, and breached its duties thereby;

g. Whether AFLAC breached its fiduciary duty to Plaintiff and the Class;

h. Whether AFLAC breached its duty of confidence to Plaintiff and the Class;

i. Whether AFLAC entered a contract implied in fact with Plaintiff and the Class;

j. Whether AFLAC breached that contract by failing to adequately safeguard Plaintiff's and Class members' Private Information;

k. Whether AFLAC was unjustly enriched;

l. Whether Defendant failed to provide notice of the Data Breach in a timely manner; and

m. Whether Plaintiff and Class members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

95. Typicality – Plaintiff's claims are typical of the claims of the members of the Class. The claims of the Plaintiff and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiff and members of the Class all had information stored in AFLAC's system(s), each having their Private Information exposed and/or accessed by an unauthorized third party.

96. Adequacy of Representation – Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the other Class members Plaintiff seeks to represent; Plaintiff has retained counsel competent and experienced in complex Class action litigation; Plaintiff intends to prosecute this action vigorously; and Plaintiff's counsel has adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class members will be fairly and adequately protected and represented by Plaintiff and Plaintiff's counsel.

97. Predominance – Defendant has engaged in a common course of conduct toward Plaintiff and Class members, in that all Plaintiff and Class member's Private Information was stored on the same computer systems and unlawfully accessed in

the same way. The common issues arising from Defendant's conduct affecting Class members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

98. Superiority – A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class members would create a risk of inconsistent or varying adjudications with respect to individual Class members, which would establish incompatible standards of conduct for AFLAC. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

99. AFLAC has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

100. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would

advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether AFLAC failed to timely and adequately notify the public of the Data Breach;

b. Whether AFLAC owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether AFLAC's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;

d. Whether AFLAC's failure to institute adequate protective security measures amounted to negligence;

e. Whether AFLAC failed to take commercially reasonable steps to safeguard consumers' and employees' Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

101. Finally, all members of the proposed Class are readily ascertainable. AFLAC has access to Class members' names and addresses affected by the Data

Breach. Class members have already been preliminarily identified and received notice of the Data Breach by Defendant.

FIRST CAUSE OF ACTION

NEGLIGENCE

102. Plaintiff restates and realleges the preceding allegations above as if fully alleged herein.

103. Plaintiff brings this claim individually and on behalf of the Class.

104. Defendant owed a duty to Plaintiff and Class members to exercise reasonable care in safeguarding and protecting their Private Information in its possession, custody, and control.

105. Defendant's duty to use reasonable care arose from several sources, including but not limited to those described below.

106. Defendant had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and Class members were the foreseeable and probable victims of any inadequate security practices on the part of the Defendant. By collecting and storing valuable Private Information that is routinely targeted by criminals for unauthorized access, Defendant was obligated to act with reasonable care to protect against these foreseeable threats.

107. Defendant breached the duties owed to Plaintiff and Class members and thus was negligent. As a result of a successful attack directed towards Defendant that

compromised Plaintiff's and Class members' Private Information, Defendant breached its duties through the following errors and omissions that allowed the Data Breach to occur:

a. mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of Private Information;

b. mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks;

c. failing to design and implement information safeguards to control these risks;

d. failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures;

e. failing to evaluate and adjust its information security program in light of the circumstances alleged herein;

f. failing to detect the breach at the time it began or within a reasonable time thereafter;

g. failing to follow its own privacy policies and practices published to its customers; and

h. failing to adequately train and supervise employees and third party vendors with access or credentials to systems and databases containing sensitive Private Information.

108. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class members, their Private Information would not have been compromised.

109. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have suffered injuries, including, but not limited to:

a. Theft of their Private Information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of their Private Information;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft

protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

g. Damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their Private Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' data; and

i. Emotional distress from the unauthorized disclosure of Private Information to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class members.

110. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SECOND CAUSE OF ACTION

NEGLIGENCE *PER SE*

111. Plaintiff restates and realleges the preceding allegations above as if fully alleged herein.

112. Plaintiff brings this claim individually and on behalf of the Class.

113. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Defendant for failing to use reasonable measures to protect ""Private Information"". Various FTC publications and orders also form the basis of Defendant's duty.

114. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of a data breach involving Private Information of its customers.

115. Plaintiff and members of the Class are consumers within the Class of persons Section 5 of the FTC Act was intended to protect.

116. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

117. The harm that has occurred as a result of Defendant's conduct is the type of harm that the FTC Act and Part 2 was intended to guard against.

118. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

THIRD CAUSE OF ACTION

BREACH OF FIDUCIARY DUTY

119. Plaintiff restates and realleges the preceding allegations above as if fully alleged herein.

120. Plaintiff brings this claim individually and on behalf of the Class.

121. Plaintiff and Class members have an interest, both equitable and legal, in the Private Information about them that was conveyed to, collected by, and maintained by Defendant and that was ultimately accessed or compromised in the Data Breach.

122. As a recipient of consumers' Private Information, Defendant has a fiduciary relationship to Plaintiff and the Class members.

123. Because of that fiduciary relationship, Defendant was provided with and stored private and valuable Private Information related to Plaintiff and the Class. Plaintiff and the Class were entitled to expect their information would remain confidential while in Defendant's possession.

124. Defendant owed a fiduciary duty under common law to Plaintiff and Class members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their Private Information in Defendant's possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

125. As a result of the parties' fiduciary relationship, Defendant had an obligation to maintain the confidentiality of the information within Plaintiff's and the Class members' records.

126. Defendant had possession and knowledge of confidential Private Information of Plaintiff and Class members, information not generally known.

127. Plaintiff and Class members did not consent to nor authorize Defendant to release or disclose their Private Information to unknown criminal actors.

128. Defendant breached its fiduciary duties owed to Plaintiff and Class members by, among other things: mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and

compromise of Private Information; mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; failing to design and implement information safeguards to control these risks; failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; failing to evaluate and adjust its information security program in light of the circumstances alleged herein; failing to detect the breach at the time it began or within a reasonable time thereafter; failing to follow its own privacy policies and practices published to its customers and employees; and failing to adequately train and supervise employees and third-party vendors with access or credentials to systems and databases containing sensitive Private Information.

129. But for Defendant's wrongful breach of its fiduciary duties owed to Plaintiff and Class members, their Private Information would not have been compromised.

130. As a direct and proximate result of Defendant's negligence, Plaintiff and Class members have suffered injuries, including:

a. Theft of their Private Information;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of their Private Information;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

g. Damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their Private Information, which remains in Defendant's possession and is

subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class members' data; and

i. Emotional distress from the unauthorized disclosure of Private Information to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class members.

131. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

FOURTH CAUSE OF ACTION

UNJUST ENRICHMENT

132. Plaintiff restates and realleges the preceding allegations above as if fully alleged herein.

133. Plaintiff brings this claim individually and on behalf of the Class.

134. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff and the Class members.

135. As such, a portion of the payments made by or on behalf of Plaintiff sand the Class members is to be used to provide a reasonable level of data security,

and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

136. Plaintiff and Class members conferred a monetary benefit on Defendant. In exchange, Plaintiff and Class members should have received from Defendant the goods and services that were the subject of the transaction and have their Private Information protected with adequate data security.

137. Defendant knew that Plaintiff and Class members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiff and Class members for business purposes.

138. In particular, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class members' Private Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class members by utilizing cheaper, ineffective security measures. Plaintiff and Class members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

139. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class members,

because Defendant failed to implement appropriate data management and security measures that are mandated by its common law and statutory duties.

140. Defendant failed to secure Plaintiff and Class members' Private Information and, therefore, did not provide full consideration for the benefit Plaintiff and Class members provided.

141. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

142. If Plaintiff and Class members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to have their information provided to Defendant.

143. Plaintiff and Class members have no adequate remedy at law.

144. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have suffered injuries, including, but not limited to:

a. Theft of their Private Information;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their Private Information;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

g. Damages to and diminution in value of their Private Information entrusted, directly or indirectly, to Defendant with the mutual understanding that Defendant would safeguard Plaintiff's and Class members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their Private Information, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to

undertake appropriate and adequate measures to protect Plaintiff's and Class members' data; and

i. Emotional distress from the unauthorized disclosure of Private Information to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiff and Class members.

145. As a direct and proximate result of Defendant's conduct, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm.

146. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class members overpaid for Defendant's services.

FIFTH CAUSE OF ACTION

DECLARATORY JUDGMENT

147. Plaintiff restates and realleges the preceding allegations above as if fully alleged herein.

148. Plaintiff brings this claim individually and on behalf of the Class.

149. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

150. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiff's and Class members' Private Information, and whether Defendant is currently maintaining data security measures adequate to protect Plaintiff and Class members from future data breaches that compromise their Private Information. Plaintiff and the Class remain at imminent risk that additional compromises of their Private Information will occur in the future.

151. The Court should also issue prospective injunctive relief requiring Defendant to employ adequate security practices consistent with law and industry standards to protect consumers' Private Information.

152. Defendant still possess Plaintiff's and Class members' Private Information.

153. Defendant has made no announcement that it has changed its data storage or security practices relating to the storage of Plaintiff's and Class members' Private Information.

154. To Plaintiff's knowledge, Defendant has made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

155. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at AFLAC. The risk of another such breach is real, immediate, and substantial.

156. The hardship to Plaintiff and Class members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another data breach occurs at AFLAC, Plaintiff and Class members will likely continue to be subjected to a heightened, substantial, imminent risk of fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

157. Issuance of the requested injunction will not compromise the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at AFLAC, thus eliminating the additional injuries that would result to Plaintiff and Class members, along with other consumers whose Private Information would be further compromised.

158. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that AFLAC implement and maintain reasonable security measures, including but not limited to the following:

a. Engaging third-party security auditors/penetration testers, as well as internal security personnel, to conduct testing that includes simulated attacks, penetration tests, and audits on AFLAC systems on a periodic basis, and ordering AFLAC to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Purging, deleting, and destroying Private Information not necessary for its provisions of services in a reasonably secure manner;

e. Conducting regular database scans and security checks; and

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify

and contain a breach when it occurs and what to do in response to a breach.

DEMAND FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all others similarly situated, demand relief as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiff as a Class Representative and his counsel as Class Counsel;

b) For equitable relief enjoining AFLAC from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class members;

c) For equitable relief compelling AFLAC to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Personal Information compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of AFLAC's wrongful conduct;

e) Ordering AFLAC to pay for not less than three years of credit monitoring services for Plaintiff and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i) Pre- and post-judgment interest on any amounts awarded; and,

j) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

A jury trial is demanded by Plaintiff on all claims so triable.

June 23, 2025

Respectfully Submitted,

/s/ *James M. Evangelista*

James M. Evangelista (GA Bar 707807)
EVANGELISTA WORLEY LLC
10 Glenlake Parkway
South Tower Suite 130
Atlanta, GA 30328
Tel.: (404) 205-8400
jim@ewlawllc.com

Jennifer Czeisler (*pro hac vice* forthcoming)
Edward Ciolko (*pro hac vice* forthcoming)
STERLINGTON PLLC
228 Park Avenue South, No. 97956
New York, New York 10003
Tel.: (212) 433-2993
jen.czeisler@sterlingtonlaw.com
edward.ciolko@sterlingtonlaw.com

Blaine Finley (*pro hac vice* forthcoming)
FINLEY PLLC
1455 Pennsylvania Avenue, NW
Suite 400
Washington, D.C. 20004
Tel.: 281-723-7904
bfinley@finley-pllc.com